

1 Randall D. Haimovici (*Pro Hac Vice Approved*)
rhaimovici@shb.com

2 Rachael M. Smith (*Pro Hac Vice Approved*)
rxsmith@shb.com

3 SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
4 San Francisco, California 94104-4505
Telephone: 415.544.1900
5 Facsimile: 415.391.0281

6 Tony M. Diab (Nevada State Bar No. 12954)
tdiab@shb.com

7 SHOOK, HARDY & BACON L.L.P.
5 Park Plaza, Suite 1600
8 Irvine, California 92614-2546
Telephone: 949.475.1500
9 Facsimile: 949.475.0016

10 Robert J.B. Flummerfelt (Nevada State Bar No. 11122)
rflummerfelt@hotmail.com

11 Rami Hernandez (Nevada State Bar No. 13146)
rhernandeznsj@hotmail.com

12 CANON LAW SERVICES, LLC
7251 W. Lake Mead Blvd., Suite 300
13 Las Vegas, Nevada 89128
Telephone: 702.562.4144
14 Facsimile: 702.866.9868

15 Attorneys for Plaintiff
MICROSOFT CORPORATION

17 UNITED STATES DISTRICT COURT

18 DISTRICT OF NEVADA

20 MICROSOFT CORPORATION,

21 Plaintiff,

22 vs.

23 NASER AL MUTAIRI, an individual;
24 MOHAMED BENABDELLAH, an individual;
25 VITALWERKS INTERNET SOLUTIONS,
LLC, d/b/a NO-IP.com; and DOES 1-500,

26 Defendants.

) Case No. 2:14-cv-00987-GMN-GWF

) **ORDER FOR PRELIMINARY INJUNCTION**

Plaintiff Microsoft Corporation (“Microsoft”) has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the Anti-Cybersquatting Consumer Protection Act (15 U.S.C. § 1125); (3) Unlawful Acts Regarding Computers and Information Services (N.R.S. § 205.4765); and (4) the common law of trespass to chattels, conversion, and negligence. Microsoft moved *ex parte* for an emergency temporary restraining order (TRO) and for an order to show cause why a preliminary injunction should not be granted pursuant to Rule 65(b) of the Federal Rules of Civil Procedure. An Amended *Ex Parte* Temporary Restraining Order and Order to Show Cause Regarding Preliminary Injunction was granted on June 26, 2014. This Court granted a Second Amended Order on June 30, 2014, and entered a TRO and Order to Show Cause against Defendants Vitalwerks Internet Solutions, LLC d/b/a No-IP.com (“Vitalwerks”), Naser Al Mutairi, Mohamed Benabdellah, and Does 1-500. Pursuant to the Second Amended Order entered on June 30, 2014, a hearing on the Order to Show Cause as to why a preliminary injunction should not issue was set for July 10, 2014, at 3:00 p.m., in LV Courtroom 7D. On July 8, 2014, Microsoft and Defendant Vitalwerks agreed to a confidential settlement, and a Stipulation of Dismissal of Defendant Vitalwerks was filed. Pursuant to the Court’s Second Amended Order, the remaining known Defendants, Naser Al Mutairi and Mohamed Benabdellah (collectively the “Malware Defendants”), were served notice of this lawsuit by e-mail, Facebook message, and by publication on a publicly-available website. Microsoft now moves for a preliminary injunction order seeking to enjoin the two Malware Defendants from creating or spreading malware of any kind and also enjoin them from teaching others how to use or spread their malware.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft’s Application for Emergency TRO and Order to Show Cause Regarding Preliminary Injunction (“TRO Motion”), the Court hereby makes the following findings of fact and conclusions of law:

1. This Court has jurisdiction over the subject matter of this case, and there is good cause to believe that it will have jurisdiction over the remaining parties; the complaint states a claim

1 upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18
2 U.S.C. § 1030), the Anti-Cybersquatting Consumer Protection Act (15 U.S.C. § 1125), Nevada's
3 Unlawful Acts Regarding Computers and Information Services (N.R.S. § 205.4765), and the
4 common law of trespass to chattels, conversion, and negligence.

5 2. Microsoft served the Malware Defendants with copies of the summons, complaint, all
6 exhibits to the complaint, the TRO, and Appendices A and B to the TRO on June 30, 2014 by e-
7 mail. Microsoft also provided notice to these Defendants by Facebook message and by publishing
8 the documents on a publicly-available website, www.noticeoflawsuit.com. This Court finds that
9 these Defendants have been given notice of the lawsuit and order to show cause hearing.

10 3. There is good cause to believe that Malware Defendants have engaged in and are
11 likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. §
12 1030), Nevada's Unlawful Acts Regarding Computers and Information Services (N.R.S. §
13 205.4765), and the common law of trespass to chattels, conversion, and negligence, and that
14 Microsoft is, therefore, likely to prevail on the merits of this action.

15 4. There is good cause to believe that, unless the Malware Defendants are restrained and
16 enjoined by order of this Court, immediate and irreparable harm will result from their ongoing
17 violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), Nevada's Unlawful Acts
18 Regarding Computers and Information Services (N.R.S. § 205.4765), and the common law of
19 trespass to chattels, conversion, and negligence because Microsoft's and its users' computers will
20 continue to be infected with and controlled by the Bladabindi/Jenxcus malware. With this malware,
21 hackers are able to control the infected computer and carry out a variety of intrusive and malicious
22 actions on the computer including logging the user's keystrokes, capturing sensitive information like
23 user names and passwords, and recording the user with the computer's video camera or microphone.

24 5. The evidence set forth in Microsoft's TRO Motion, the accompanying declarations
25 and exhibits, and supplemental declarations that have been submitted to this Court, demonstrates that
26 Microsoft is likely to prevail on its claim that the Malware Defendants have engaged in violations of
27 the foregoing laws through one or more of the following:
28

- a. Intentionally and knowingly accessing and sending malicious code to the protected computers and operating systems of Microsoft and its customers without authorization, in order to infect those computers and intending to cause damage and benefiting therefrom;
- b. Sending malicious code to access the protected computers without authorization or in excess of any authorization to control and/or obtain information from the computers;
- c. Delivering malicious code;
- d. Knowingly, willfully, and without authorization publishing and transferring malware to Doe Defendants; and
- e. Negligently engaging in such acts and permitting, enabling and encouraging other defendants to participate in illegal acts harmful to Microsoft, Microsoft's customers, and the general public.

6. There is good cause to believe that if such conduct continues, irreparable harm will occur to Microsoft, its customers, and the public. There is good cause to believe that the Malware Defendants will continue to engage in such unlawful actions if not immediately restrained from doing so by Order of this Court.

7. There is good cause to permit notice of this Order by alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due Process and Federal Rule of Civil Procedure 4(f)(3), and are reasonably calculated to notify Defendants of the Order:

- (1) transmission by e-mail and/or Facebook on the Malware Defendants; and
- (2) publishing notice on a publicly available Internet website.

8. There is good cause to believe that the harm to Microsoft by denying the relief requested in its request for a Preliminary Injunction outweighs any harm to any legitimate interest of Defendants and that there is no undue burden to any third party.

PRELIMINARY INJUNCTION

IT IS THEREFORE ORDERED as follows:

A. The Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from intentionally accessing and sending malicious software or code to Microsoft's and its customers' computers and operating systems, without authorization, to infect those computers with the Bladabindi/Jenxcus or other malware.

B. The Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from communicating with, accessing, remotely controlling, collecting data or information from, sending commands to, and/or downloading additional malware onto the infected computers.

C. The Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from intentionally creating and/or spreading new or updated versions of the Bladabindi/Jenxcus malware or other malware that can be used to access or control Microsoft's and its customers' computers and operating systems without authorization.

D. The Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from making malware available for others to use or download.

E. The Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from teaching, instructing, or educating others on how to use or spread the malware the Malware Defendants created. This includes, but is not limited to, enjoining these Defendants from posting online tutorials on how to use or spread the malware.

IT IS FURTHER ORDERED that, the Malware Defendants, their representatives, and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the spread of the Bladabindi, Jenxcus, or other malware, or other malware-related activity including communicating

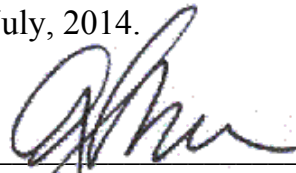
1 with infected computers through the domains set forth in Appendix A or through any other domain
2 leased, registered, or hosted by, or otherwise obtained from, Vitalwerks Internet Solutions, LLC
3 d/b/a No-IP.

4 **IT IS FURTHER ORDERED** that copies of this Order may be served by any means
5 authorized by law, including by means previously authorized for the complaint and TRO in the
6 Second Amended Order issued by this Court on June 30, 2014.

7 **IT IS FURTHER ORDERED** that this Order shall remain in effect until the case is resolved
8 by dismissal of the complaint, judgment, or other final decree against the Defendants enjoined by
9 this Order,

10 **IT IS FURTHER ORDERED** that Microsoft shall maintain its bond in the amount of
11 \$200,000 that it has paid to the Court Clerk until this case is resolved.

12 **IT IS SO ORDERED** this 10th day of July, 2014.

13
14 
15 _____
16 Gloria M. Navarro, Chief Judge
17 United States District Judge
18
19
20
21
22
23
24
25
26
27
28